To: Justice Information Board Members and Designees

From: Brian LeDuc, Program Director

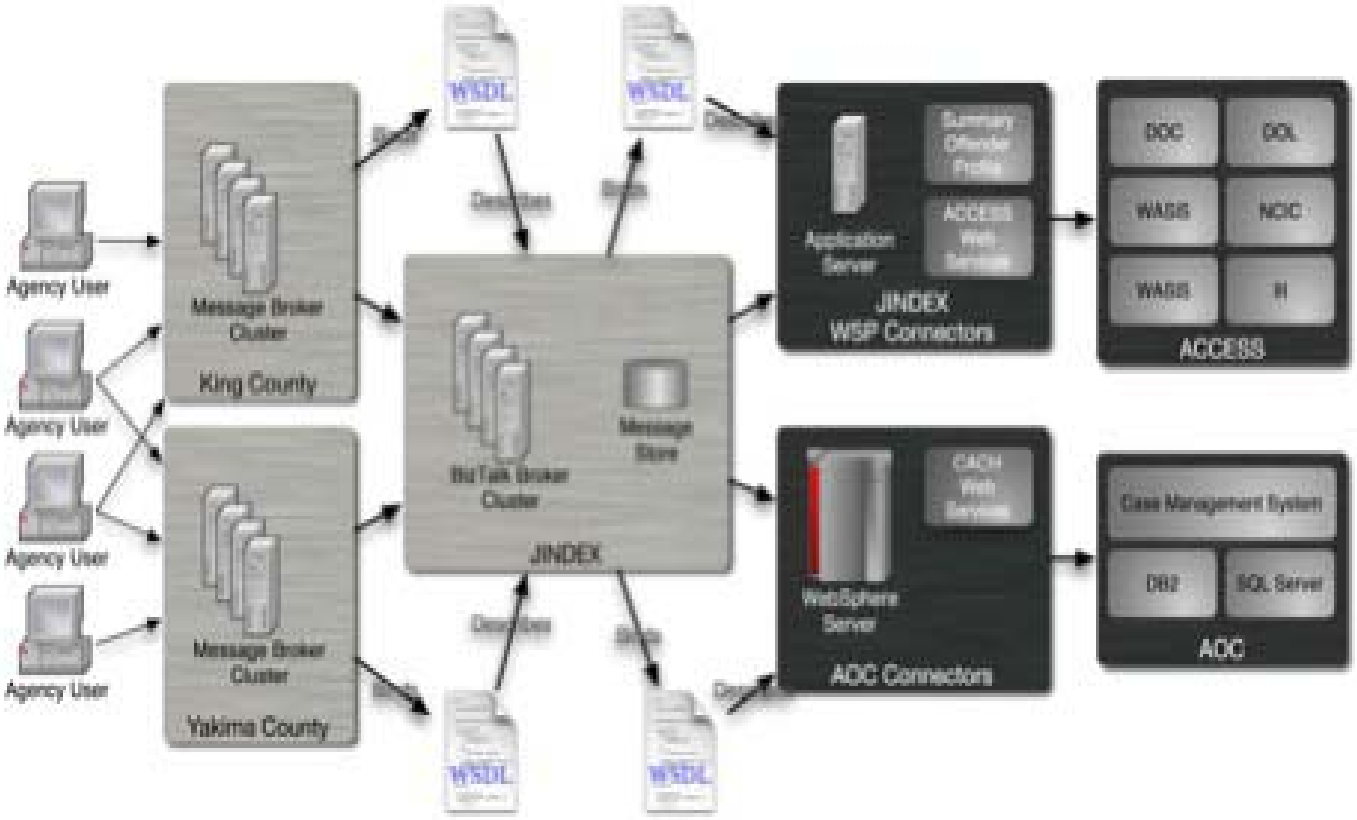
Date: 3/11/2005

Re: Report of the Program Director, February 15–March 14, 2005

Justice Information Data Exchange (JINDEX)

I have submitted an Acquisition Plan for the JINDEX Hardware and Software through DIS, and hope to have it installed this month.

The Baseline Requirements deliverable has been finalized, after review and comment by the Technical Advisory Group. The document expands upon the requirements outlined in the Customer Requirements Report based on follow-up stakeholder interviews and Technical Advisory Group (TAG) meetings. A Design Document deliverable will follow. The Baseline Requirements document contains measurements for Critical Success Factors and a clear outline of what is to be delivered during the implementation phase. A full copy is included as Attachment A to this report. The high level architecture is displayed below:



The next month will see finalization of the design for JINDEX and the CACH query, as well as installation and configuration of the hardware and software. It is important to note that support for this model is contingent upon passage of the DIS Budget Request for JIN.

Summary Offender Profile (SOP)

Templar is currently working to correct a problem with the application's connectivity to AOC. It is worth noting that it was a year ago that the application was deemed ready for deployment and handed over to the Program Office. It has never actually worked, with problems ranging from parsing errors to hitting the incorrect server at courts to the current performance problem.

A summary of the project, including the lessons to be gained from the experience is included at Attachment B.

E-Citations

HB 1650 and SB 5627, the bills to eliminate the requirement that officers collect signatures when issuing citations, continue to move sluggishly through the process. After amendments suggested by the Association of Washington Cities were incorporated (preserving the requirement that signatures are gathered for paper tickets), the bills are respectively on the House floor and in the Senate Rules Committee. Representative Darneille offered an amendment to the House bill on Thursday March 10 articulating the right of the accuse to challenge the accuracy of an officer's identification at a hearing. At this time, everyone appears to find this amendment acceptable except WASPC, and we have not yet had a chance to hear their position.

On the operations side, I am planning to issue a request for proposals on March 21 to design the architecture for electronic citations and automate the Law Enforcement→Courts→Depatment of Licensing exchange, using the Law Enforcement Suport Agency (LESA) as a pilot. This project will help to validate the JINDEX model and will create a second service using the integration platform. A statement of work for the project is included as Attachment C.

FY 2005 Grants

At the last meeting, the Board asked me to consult the Technical Advisory Group to review proposals for FY 2005 NCHIP and JAG (formerly Byrne) grants. I developed a 2005 Decision Package and posted an announcement to the JIN web site on February 18, with applications due by March 5.

The current funding for this year is $290,000 for JAG and $697,000 for NCHIP, although some of this will be absorbed by administrative costs at OFM (they declined to provide a figure). We received three proposals—two of which were submitted by the deadline: one from the JIN Program Office to add services to the JINDEX ($350,000) and one from King County to develop a web service interface for warrants data, using the JINDEX architecture. On March 11, we received a proposal from the WSP for $896,000, to be used for Livescan machines. All three proposals are included as Attachment D to this report.

1) The TAG will review these proposals on Tuesday March 15 before the Board meeting and provide recommendations for subsequent discussion.

ACTION

Approve or modify recommendations for the allocation of 2005 NCHIP and JAG funds.

ATTACHMENT A

Washington Justice Information Network
Case and Criminal History (CACH)
Query Project
Requirements Baseline

February 18, 2005

Version 10

Online
BUSINESS SYSTEMS

Online Business Systems
One World Trade Center
121 SW Salmon St.
Portland, Oregon 97204

Document History

Version	Date	Author	Comments
10	23 Feb 2005	AR	Incorporated JIN Program Director's review comments into document structure, moving Funding Recommendations into a separate document.
11	3 Mar 2005	AR	Incorporated Stakeholder feedback

Table of Contents

1 INTRODUCTION

1.1 DOCUMENT PURPOSE

This document expands upon the JINDEX and CACH requirements outlined in the approved Customer Requirements Report. Follow-up stakeholder interviews and Technical Advisory Group (TAG) meetings have clarified delivery expectations for the integration framework and the specific web service queries. While project design discussions have already been started, this document remains focused on requirements rather than design (i.e. the "what", not the "how"). A Design Document deliverable will follow this document, capturing all design decisions and discussions that have been made.

This document also contains measurements for Critical Success Factors. Traceability is provided between the newly-introduced technical requirements and the functional requirements, which were originally presented in the Customer Requirements Report. The technical requirements provide additional detail to the Functional Requirements, manage scope, and should all be stated in language that facilitates testing and verification of conformance. In essence, this Requirements Baseline should make it clear exactly what is to be delivered during the implementation phase of the CACH project.

1.2 RELATED ARTIFACTS

Artifact	Description
Contract A04-PSC-007	Contract between State of Washington DIS and Online Business Systems dated 1Nov2004.
Statement of Work	JIN SOW – Exhibit A within Contract A04-PSC-007. Defines detailed success criteria, deliverables and work expectations.
Online Proposal	Online Business Systems technical proposal (Volume 1) to Washington DIS in response to RFP # A04-RFP-005. Contains the Overall Online approach being used on the project.
JINDEX CACH Project Charter V12	Approved Project Charter.
JINDEX CACH Customer Requirements Report V29	Approved Customer Requirements Report.
JINDEX CACH Alternatives Document V4	Design Alternatives – In-Progress.

1.3 DISTRIBUTION

Brian LeDuc	State of Washington – JIN Program Director
Andy Ross	Online Business Systems Ltd. – Senior Solutions Architect / JIN CACH Project Manager
Dave Usery	URL Integration Ltd. – Integrated Justice Domain Business Analyst
David Neufeld	Online Business Systems Ltd. – Delivery Manager

2 CRITICAL SUCCESS FACTORS

The Critical Success Factors, as presented in the Customer Requirements Report, are explored in greater detail in this section. In addition, a set of recommended success measurement criteria is noted for each Factor. These measurement criteria are not intended to define the scope of the JINDEX CACH Project but instead, to advise the JIN Program Office on techniques whereby the success of the Program can be measured and managed overall.

J I N D E X	
#	**Critical Success Factor**
CSF2	**Increased awareness of Criminal Justice service availability.** A central role for the JIN Program Office will be to promote the availability of criminal justice services, and provide support for jurisdictions who are interested in participating in those services. It will require a commitment of JIN Program Office resources in providing outreach through meetings and other information dissemination tools to make local jurisdictions in Washington State aware of the availability of such services. In addition, it will require a commitment of time for JIN Program Office staff in working with each local jurisdiction's project managers to resolve any technology issues related to information sharing. Clearly defining what services JINDEX will provide in the near term as well as over the long term is essential. If the services are not clear, there is the risk of expectations being too high or so low as to not generate interest. An essential first step in communicating what benefits of JINDEX CACH services is dependent on understanding what the services are. The JIN Program Office's role of defining how justice agencies will exchange information is clear, in that it is the Office's responsibility to facilitate the development and dissemination of the framework. What also must be well-defined and communicated is what services the JIN Program Office will provide beyond the framework. The registry of web services that JINDEX will either expose or maintain is a significant factor in the success of the reply/response exchanges. The range of services that JINDEX may eventually make available through the central registry must be clearly articulated. If the assumption is that all of the non-functional requirements defined for JINDEX will be met in the framework design and ultimately the resulting standards, then there must be a common awareness, understanding and acceptance of what of these services the JIN Program Office will maintain and which will be simply supported through coordination and standard setting. The partner agencies minimally must understand that if the standards are not adhered to it will not be possible to register the services with JINDEX. Recommended Success Measurement Criteria: 1. Number of Integration Project Deliverables where JINDEX is considered or named. 2. Number of hits to the JIN website. 3. Number of Agencies made aware of the services through direct communication. 4. Number of speaking/presentation engagements conducted where JINDEX services are highlighted. 5. Response to annual user/agency satisfaction survey (including opportunity to propose changes & enhancements to the system)

J I N D E X	
#	**Critical Success Factor**
CSF5	**Criminal Justice Agencies increase solution delivery effectiveness by leveraging SOA best-practices and examples.** Another important role for the JIN Program Office will be to provide general information and training to local jurisdictions about the importance of standards and service oriented architecture, and how use of these tools and best practices can improve the readiness of local agencies to participate and interoperate with other Agencies using the JINDEX adopted standards. In doing so, the JINDEX architecture design must adhere to SOA best practices to the degree possible and have a mechanism to remain compliant as these standards evolve. The acceptance of any proprietary solutions where WS-I standards are available needs to be critically examined to ensure this does not limit the JINDEX architecture to a standard that is bound to a single vendor outside of the evolving SOA and SOAP standards. If a standard is accepted that is outside the WS-I stack, then a clear migration path to eventually embrace the WS-I standard and replace the proprietary solution is critical. The solution will include a vendor provided hub, this is a given but this must not bind the JIN to the vendor's unique solution. Recommended Success Measurement Criteria: 1. Number of Requests for JINDEX Reference Architecture. 2. Time saved or ease of utilization through testimonials received from Agencies using JINDEX Reference Architecture.
CSF6	**Criminal Justice Agencies design / deliver solutions and projects that use or consider JINDEX principles.** JIN outreach and training must include the ability of the Program Office to provide assistance to local project managers in ensuring these projects consider the JIN Integration Framework principles. Recommended Success Measurement Criteria: 1. Number of new compliant JINDEX Services added to the Registry. 2. Number of Integration Project deliverables that make interoperability statements regarding JINDEX.

The following table outlines the Critical Success Factors related to the second aspect of this project, the query services themselves.

JINDEX CACH Services	
#	**Critical Success Factor**
CSF 1	**AOC Case and WSP Criminal History repository information consumable as a web service.** There are specific criteria necessary to make AOC and WSP information consumable as a JINDEX web service. The AOC is undergoing major changes and updates to their legacy systems, to make them more available and accessible to existing users and a broader, statewide integration effort. The AOC effort is moving the existing JIS and six other enterprise systems to a series of web applications, consistent with AOC application architectural standards. The WSP priority is to use a fully Washington-compliant XML transaction between state central and customer applications/regional interface for all transactions in the WS access switch. The JINDEX query service will need to accommodate these existing initiatives and priorities to ensure information availability. Recommended Success Measurement Criteria: 1. Total number of distinct successful request/reply message conversations. 2. Reduced number of failed access attempts.
CSF 3	**King County users are delivered Integrated Justice information through web services interface.** King County is already implementing its own regional justice information sharing system through its integration hub. It is a sophisticated effort, using web services and other middleware technology. As such, the JIN web services interface will need to work with the King County LOWS (local objects and web services) structure to extend the current functionality of King County systems and allow these systems to fully participate in the JINDEX query service. Recommended Success Measurement Criteria: 1. Number of King County success request/reply message conversations. 2. Number of King County users accessing JINDEX CACH Web Services.
CSF 4	**Yakima County users are delivered Integrated Justice information through web services interface.** Recommended Success Measurement Criteria: 1. Number of Yakima County success request/reply message conversations. 2. Number of Yakima County users accessing JINDEX CACH Web Services.

3 TECHNICAL REQUIREMENTS

3.1 DATA MODEL

3.1.1 JINDEX

As a guiding principle, JINDEX will use the Global Justice XML Data Model (GJXDM) for all XML-based data exchanges. As such, GJXDM can be considered as the defacto JINDEX Data Model, the Common Business Format, and the canonical model for any implemented services.

3.1.2 CACH Query Services

CACH Query Services will interface with two data repositories, the Administrative Office of the Courts (AOC) and the Washington State Patrol (WSP). For each data repository, two separate query services will be enabled: (1) an ID of possible match query, and (2) the Case and Criminal History Query. The following identifies the technical requirements for each of these queries, pertaining specifically to the conceptual/logical data model. Note that this is conceptual only; the objective is to identify data elements necessary for the queries, not to name or structure them according to specific conventions.

#	Technical Requirement
T1	Authorization to obtain records via the National Crime Information Center (NCIC) Interstate Identification Index (III) is governed by federal laws and state statutes approved by the U. S. Attorney General that are applicable to the U.S. Department of Justice, Federal Bureau of Investigation, and NCIC 2000. As such, all requests for information through CACH Query Services shall include: • The Originating Agency Identifier (ORI) from which the request is generated, and • A valid Purpose Code
T2	While not required by law and statute, all requests for information through CACH Query Services shall also include: • The name of the individual within the criminal justice agency requesting the information This has been identified by the State Patrol as a likely future requirement for NCIC and III. It will also assist in debugging and auditing.

<table>
<tr><th>#</th><th>Technical Requirement</th></tr>
<tr><td>T3</td><td>The ID of Possible Match Query will allow a Criminal Justice Practitioner to query on a person's characteristics and attributes, in order to determine if the person exists in existing Court and/or Criminal data repositories. Possible inputs into this query include:
<table>
<tr><th>Person</th></tr>
<tr><td>Name (first, middle, last)</td></tr>
<tr><td>FBI Number</td></tr>
<tr><td>State Identification Number</td></tr>
<tr><td>Driver's License Number</td></tr>
<tr><td>Social Security Number</td></tr>
<tr><td>PCN</td></tr>
<tr><td>Other Identification Number (e.g. passport, military ID)</td></tr>
<tr><td>Date of birth</td></tr>
<tr><td>Sex</td></tr>
<tr><td>Race</td></tr>
<tr><td>Address</td></tr>
<tr><td>City</td></tr>
<tr><td>State</td></tr>
<tr><td>ZIP Code</td></tr>
</table>
Because the Criminal Justice Practitioner will likely have incomplete information on a subject, all of these parameters will be optional in the query. This will allow for very flexible querying based on a wide range of inputs (e.g. "Joe Perp, Caucasian, Male", "Jane Doe, Hispanic, Female, Tacoma, WA", etc.)</td></tr>
<tr><td>T4</td><td>The ID of Possible Match Query will use the input Name fields to automatically query against backend systems' Name and Alias fields, without requiring the service consumer to explicitly denote aliases in the request.</td></tr>
</table>

<table>
<tr><th>#</th><th>Technical Requirement</th></tr>
<tr><td>T5</td><td>Outputs of the ID of Possible Match Query will include all of the same data elements as the query input, as well as the source of the record. Note that this response does not include PCN, since a single subject may have multiple PCNs.
<table>
<tr><td>Person</td></tr>
<tr><td>Name (first, middle, last, suffix)</td></tr>
<tr><td>Aliases (first, middle, last, suffix)</td></tr>
<tr><td>FBI Number</td></tr>
<tr><td>State Identification Number</td></tr>
<tr><td>Driver’s License Number</td></tr>
<tr><td>Social Security Number</td></tr>
<tr><td>AOC Identifier</td></tr>
<tr><td>Other Identification Number (e.g. passport, military ID)</td></tr>
<tr><td>Date of birth</td></tr>
<tr><td>Sex</td></tr>
<tr><td>Race</td></tr>
<tr><td>Address</td></tr>
<tr><td>City</td></tr>
<tr><td>State</td></tr>
<tr><td>ZIP Code</td></tr>
<tr><td>Scars, Marks and Tattoos</td></tr>
<tr><td>Eye Color</td></tr>
<tr><td>Hair Color</td></tr>
<tr><td>Height</td></tr>
<tr><td>Weight</td></tr>
<tr><td>Record Source</td></tr>
</table>
This will allow the Criminal Justice Practitioner to determine the appropriate record(s) that corresponds most closely to the subject on whom they are querying. For example, if the Criminal Justice Practitioner queries on Joe Perp, Caucasian, Male”, the result might be a lengthy list such as:
<table>
<tr><td>Name</td><td>State #</td><td>Address</td><td>City</td><td>State</td><td>Source</td></tr>
<tr><td>Joe Perp</td><td>11111</td><td>123 Main St</td><td>Olympia</td><td>WA</td><td>AOC</td></tr>
<tr><td>Joe Perp</td><td>22222</td><td>456 9th Ave</td><td>Seattle</td><td>WA</td><td>AOC</td></tr>
<tr><td>Joe Perp</td><td>22222</td><td>456 9th Ave</td><td>Seattle</td><td>WA</td><td>WSP</td></tr>
<tr><td>…….</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Joe Perp</td><td>99999</td><td>789 1st St</td><td>Portland</td><td>OR</td><td>NCIC</td></tr>
</table>
</td></tr>
</table>

#	Technical Requirement
T6	The CACH Query will allow a Criminal Justice Practitioner to 'drill in' to a person's specific records in Court and/or Criminal data repositories. Possible inputs into this query include: FBI Number State Identification Number Driver's License Number Social Security Number AOC Identifier Other Identification Number (e.g. passport, military ID) PCN Criminal Justice Practitioners will only need to supply *one* of the identification numbers in order to execute this query; however, the provision of all available identifiers will increase the likelihood of getting the best possible dataset back.
T7	While the PCN is 'incident' rather than 'person' based (i.e. a single person may have multiple PCNs), stakeholders felt that Criminal Justice Practitioners would want the option to "find me all records for the person associated with this incident/PCN". As such, CACH queries will be executable based on PCN.

<table>
<tr><th>#</th><th>Technical Requirement</th></tr>
<tr><td>T8</td><td>Outputs from the CACH Query will include specific case and/or criminal history data from the Courts' and the State Patrol's data repositories. The intent is not to supply comprehensive information, with all information on every case and conviction, but to provide summary data sufficient for immediate needs and further drill down, if required (if the Criminal Justice Practitioner wishes to receive comprehensive information on a specific case or conviction, a future web service would allow further drill down, based on identification numbers). As such, the CACH Query will have the following outputs:
<table>
<tr><th>AOC / Case Info</th></tr>
<tr><td>PCN</td></tr>
<tr><td>Charge Identification Number</td></tr>
<tr><td>Charge Name</td></tr>
<tr><td>Charge Date</td></tr>
<tr><td>Charge Description</td></tr>
<tr><td>Charge Disposition</td></tr>
<tr><td>Court Name</td></tr>
<tr><td>Supervision</td></tr>
<tr><td>Sentence (optional)</td></tr>
</table>
<table>
<tr><th>WSP / Criminal Info</th></tr>
<tr><td>PCN</td></tr>
<tr><td>Charge Identification Number</td></tr>
<tr><td>Charge Name</td></tr>
<tr><td>Charge Date</td></tr>
<tr><td>Charge Description</td></tr>
<tr><td>Charge Disposition</td></tr>
<tr><td>Arresting Agency Name</td></tr>
<tr><td>Mentally Ill Status (if possible)</td></tr>
<tr><td>Chemically Dependent Status (if possible)</td></tr>
<tr><td>Violent Offender Status</td></tr>
<tr><td>Armed and Dangerous Status</td></tr>
<tr><td>Registered Sex Offender Status</td></tr>
<tr><td>Person of Interest Status, including name, date, issuing agency</td></tr>
<tr><td>Protection Order(s), including name, date, issuing agency</td></tr>
<tr><td>Warrant(s), including name, date, issuing agency</td></tr>
</table>
</td></tr>
</table>

3.2 GJXDM SUBSETTING

Functional Requirement FR9 from this project states "*All requests and replies will consist of a SOAP message with an embedded Justice XML document in the SOAP body*".

GJXDM is an all-encompassing, comprehensive standard. Unfortunately, this has resulted in the manifestation of several problems when working with the schemas. Simply put, the schemas are too large to work in most XML tools and integration servers.

From the Department of Justice – Office of Justice Program's website (http://it.ojp.gov/),

> *The Global JXDM is a reference model. This means it is not a rigid standard that must be used exactly as it is in its entirety. The Global JXDM was designed as a core set of building blocks that are used as a consistent baseline for creating exchange documents and transactions within the justice community. While an XML Schema rendering of the entire model exists, it is not a requirement for Global conformance that this entire schema be used for validation.*
>
> *The Global JXDD has grown to accommodate the needs of a large and varying user base. Though a large dictionary in itself is not a problem, users can experience difficulties when using the large XML schema generated from the full dictionary. In many practical use cases, only a subset of the full Global JXDD is required. Likewise, it is possible to validate with a reduced set (a subset) of the Global JXDM components.*
>
> *Realizing that the rules for manually creating a Global JXDM Schema Subset can be daunting and potentially error-prone, an online tool that can automatically generate a correct Schema Subset has been developed.*

From the Georgia Tech Research Institute website *(http://justicexml.gtri.gatech.edu/customized_schemas.html),*

> *A schema subset is an extraction of the full Justice dictionary. Instead of using a full schema that defines everything from the dictionary, users can use customized schema subsets that defines only those components from the JXDD that they want. This schema subset defines nothing new; everything within the subset is already defined in the dictionary.*

#	Technical Requirement
T9	JIN CACH will create GJXDM schema subsets in accordance with rules and conventions set forth by the Department of Justice – Office of Justice and Georgia Tech Research Institute.
T10	CACH GJXDM schema subsets will exist within a namespace specific to the State of Washington JIN program. This namespace may import elements from other namespaces, as determined during project design.
T11	Artifacts recommended by the GJXDM Information Exchange Package Description Guidelines, dated January 24, 2005, will be produced as part of the CACH project in order to produce consistent documentation and models for future JIN projects.

3.3 REQUEST / REPLY PATTERNS

CACH queries must take a single request from a Criminal Justice Practitioner, and broker the request to multiple sources – in this case, the AOC and the WSP. As such, a *Splitter* component is required.

Responses will be received from the AOC and ACCESS asynchronously (from the original request), at different times (from each other), and with no guarantee of the order in which they will be received. Additionally, ACCESS interfaces with multiple systems (e.g. NLETS, III, WASIS, WASIC), each of which will respond separately and asynchronously to a query. The JINDEX should, therefore, implement an *Aggregator* component to combine the AOC and multiple ACCESS responses into a single response, to be sent back to the requestor. The Aggregator component is not essential, since aggregation functions could be delegated to service consumers. For example, King and Yakima counties could each write their own Aggregators, according to their specific needs and presentation requirements. As more consumers begin using the JINDEX services, however, the delegation of aggregation functionality to individual agencies would cause multiple local re-writes of ostensibly identical business functions. It is therefore recommended that JINDEX implement an Aggregator for CACH services, and return a single response to all consuming agencies.

JIN stakeholders have indicated that CACH services should provide *all* information from the different data

repositories back to the Criminal Justice Practitioners. While some information may be repeated across responses from the different systems, CACH services should not attempt to eliminate information based on suspected duplicates. This will ultimately allow the Justice Practitioner, rather than an automated IT system, to decide what information is relevant. The Aggregator, therefore, should simply *combine* the responses from ACCESS and the AOC, rather than trying to logically tie individual records from the different systems together.

In a long running conversation where multiple responses must be aggregated together, *completion conditions* need to be defined. While there are several paradigms that may be implemented for completion conditions, the two most applicable for CACH include *Time-to-Live (TTL),* and *Number of Responses*. A TTL completion condition would dictate to the aggregator to respond, for example, in 10 seconds, no matter how many responses had been received. A Number of Responses completion condition would tell the aggregator not to respond until it had received responses from all, or a designated number of the possible providers (e.g. AOC, NLETS, III, WASIS, WASIC, DOL, DOT, and DOC). A combination of these paradigms is recommended for CACH.

Splitters and Aggregators require several components in message construction, and request/reply patterns. Request messages must have *message identifiers*, which are unique by requesting agency (e.g. King and Yakima counties may each send message #12345, but message #56789 sent twice from the same agency would be treated as a duplicate or a resend). In order to aggregate multiple, asynchronous responses, the JINDEX must statefully process *conversations*. Responses must contain *correlation identifiers*, which match the original message identifiers. As well, requests may contain a *return address* to which replies should be sent.

The following request/reply example illustrates:

1. King County sends request #12345 to the JINDEX with return address" www.kingcounty.gov"
2. JINDEX brokers request #12345 to the AOC
3. JINDEX brokers request #12345 to the WSP
4. Response from the WSP is sent to the JINDEX, with correlation id #12345
5. Response from the AOC is sent to the JINDEX, with correlation id #12345
6. Since the JINDEX has statefully processed this conversation, it aggregates all responses for correlation id #12345, and sends back a single message to the return address www.kingcounty.gov

#	Technical Requirement
T12	CACH queries will implement a *splitter* component, which will take a single request from a service consumer and split the request into multiple requests to the service providers
T13	CACH queries will implement an *aggregator* component, which will combine multiple responses related to a single request into a single response. The aggregator will combine multiple responses from different systems into a single response, but will *not* perform logical manipulation or duplicate suppression of the data contained therein.
T14	The aggregator will have administrator-configurable Time To Live and Number of Responses parameters. These will be changeable by JINDEX system administrators without requiring programming.
T15	Negative responses will be explicitly identified in responses to consumers. Negative responses will distinguish between (1) system unavailable, (2) response is still pending, and (3) system has no data to match the query
T16	The splitter and aggregator will allow for transmission and tracking of message identifiers, correlation identifiers, and return addresses.

3.4 SOAP HEADERS

SOAP is one of the three foundations of a Web Services solution – in addition to WSDL and UDDI (although the

latter is frequently omitted in real-life implementations). SOAP is the standard for web service messages. By design, SOAP is effectively an envelope expressed in XML that contains a header and message body. All messages that use the JINDEX as the service component must use SOAP.

The SOAP body contains the data that is to be processed by the web service. The content of the SOAP body will be specified by the WSDL documenting the web service. The SOAP headers contain processing information and further features of the SOAP Message. While the SOAP body is mandatory, the headers are not. However, header information may be required by a web service to complete processing. If any expected SOAP headers are not found or if the headers are not well formed, the web service must reject the message with an appropriate SOAP fault. Use of the fault message is described in the Error Handling requirements.

It should be noted that protocol level headers should be expressed in the SOAP header. While it is a requirement to use HTTP as the transport for this iteration, not all transports support header values. Using SOAP instead of a protocol level header allows other web transports to be used just as effectively as HTTP. For example, while HTTP and SMTP support header values, FTP does not. FTP remains a common method of exchange.

Most Web Service standards use SOAP headers to add features that are required in web services in a standardized fashion. Generally, the use of custom defined SOAP header element reduces the interoperability capability of Web Services.

#	Technical Requirement
T17	The following fields are required and should be expressed as part of the SOAP headers. • Security Token for WSP – ORI • Message Identifiers • Correlation Identifiers • Return Address
T18	WS-Security standards shall be used for conveying security tokens
T19	WS-Addressing standards shall be used for conveying the message identifiers, correlation identifier and the return address.

3.4.1 WS-Security

While WSS is not presently required for its privacy and integrity features, it is useful for expressing the user who is invoking the web service.

The following example is from OASIS's "Web Services Security Username Token Profile 1.0" documentation. It is used to describe how a web service can supply a Username Token as a means of identification.

```
<S11:Envelope xmlns:S11="..." xmlns:wsse="..." xmlns:wsu= "...">
<S11:Header>
  ...
        <wsse:Security>
           <wsse:UsernameToken wsu:Id=”ORI”>
              <wsse:Username>NNK</wsse:Username>
              <wsse:Password Type="...#PasswordDigest">
                 weYI3nXd8LjMNVksCKFV8t3rgHh3Rw==
              </wsse:Password>
              <wsu:Created>2003-07-16T01:24:32Z</wsu:Created>
           </wsse:UsernameToken>
        </wsse:Security>
        ...
     </S11:Header>
     ...
</S11:Envelope>
```

This example demonstrates a simple username/password combination, but the password is not a required field. The "wsu:Id" attribute on the Username Token identifies this security token as the ORI that is required by WSP.

3.4.2 WS-Addressing

While the WS-Address specification has not been ratified at the time of this document, it can be considered mature for the required fields. The goals of the WS-Address specification align with the goals of the Washington JIN Initiative.

The following is an example of a Request message with WS-Addressing header information

```
<S:Envelope xmlns:S="http://www.w3.org/2003/05/soap-envelope"
                xmlns:wsa="http://www.w3.org/@@@@/@@/addressing">
<S:Header>
   <wsa:MessageID>
         http://kc.wa.gov/6B29FC40-CA47-1067-B31D-00DD010662DA
   </wsa:MessageID>
   <wsa:ReplyTo>
      <wsa:Address>http://kc.wa.gov/JILS</wsa:Address>
   </wsa:ReplyTo>
   <wsa:To>http://jindex.wa.gov</wsa:To>
   <wsa:Action>http://jindex.wa.gov/CACHQuery</wsa:Action>
</S:Header>
<S:Body>
   ...
</S:Body>
</S:Envelope>
```

The response message would look like:

```
<S:Envelope
  xmlns:S="http://www.w3.org/2003/05/soap-envelope"
  xmlns:wsa="http://www.w3.org/@@@@/@@/addressing">
  <S:Header>
    <wsa:MessageID>
      http://jindex.wa.gov/5C25GQ09-GH14-5839-B93U-23GH987255VB
    </wsa:MessageID>
    <wsa:RelatesTo>
      http://kc.wa.gov/6B29FC40-CA47-1067-B31D-00DD010662DA
    </wsa:RelatesTo>
    <wsa:To S:mustUnderstand="1">
      http://kc.wa.gov/JILS
    </wsa:To>
    <wsa:Action>http://kc.wa.gov/JILS/processCACHQueryResponse</wsa:Action>
  </S:Header>
  <S:Body>
    <jin:CACHResponse xmlns:jin="http://jindex.wa.gov"/>
  </S:Body>
</S:Envelope>
```

3.5 LOGGING

Logging and auditing are primarily the responsibility of endpoint agencies (i.e. consumers, like King and Yakima counties, and producers, like the AOC and WSP). Presently, agencies applications already have their own logging and auditing mechanisms and these will continue to be used.

While not mandated to do so, JINDEX will provide logging functions to assist in debugging and inter-agency auditing functions. Generally, a centralized logging service with its own secure repository should be used to store logs. Then the middleware infrastructure can be leveraged to keep logging as loosely coupled as possible.

The logging framework provides the foundation for Monitoring and Error Handling. Monitoring events should be logged as well as exception events. Monitoring may uncover communication issues that need to be escalated and communicated to DIS through a notification framework. Monitoring and exception events may also need to be returned to the source agency application.

As outlined in the Customer Requirements Report Non Functional Requirement NFR19, logging too much information can rapidly deplete the storage available on a middleware server. Based on JINDEX' expected message traffic (including future web services), JINDEX logs could grow by 64 gigabytes per month if the entire contents of individual messages were captured to the logs. As such, it is recommended that JINDEX only capture a subset of message information, sufficient to facilitate debugging and auditing.

#	Technical Requirement
T20	JINDEX will log information pertaining to WHO accessed WHAT, and WHEN they did it. As such, for ID of Possible Match and CACH Requests and Responses, JINDEX will extract from the messages and log: • The agency initiating the post (e.g. this will be KC or Yakima for requests, AOC or WSP for responses) • ORI • Username • Date and time of the post • Message identifier • Correlation identifier • Return address • Type of message (e.g. ID of Possible Match Request or Response, CACH Request or Response, eCitations or future message types) Note that the contents messages will *not* be persisted. Logging this level of information will allow JINDEX administrators to support the community in determining the nature of the traffic that was routed through the framework, but not the contents of the traffic.
T21	Access to JINDEX logs will be limited by Access Control Lists (ACLs). JINDEX administrators will be the only personnel in these ACLs.
T22	Endpoint agencies will continue the current activities which facilitate compliance with established audit requirements and agreements.

3.6 MONITORING

Error handling is the process of dealing with error conditions in a process. It is the direction of all error handling processes to plan on handling anticipated errors and creating a workflow to attempt to recover.

It is desirable that no messages be lost on the JINDEX. In the event of an error, the message or request should still exist and possibly be reintroduced into a workflow. JIN stakeholders have stated, however, that there is no requirement to implement Reliable Messaging for the initial CACH query services.

The severity of an exception dictates how it is to be handled. It can be assumed that errors might be known and anticipated, even ignored while others are not anticipated and require special handling and reprocessing. Exceptions can occur at various layers of the technology stack, starting from the physical network layers up to the various software layers. Exceptions at each level must be planned for.

#	Technical Requirement
T23	JINDEX will facilitate the logging of *exception events*, such as endpoint system unavailability, mal-formed incoming messages, etc. Exception events shall be separately distinguishable from normal traffic in the JINDEX (this will likely be specific to the specific platform selected for the JINDEX and its associated tools/management consoles)
T24	For ID of Possible Match and CACH queries and responses, if an endpoint system is unavailable at the time when the JINDEX attempts to initiate a post, the JINDEX will *not* attempt to retransmit.
T25	Depending on the native functionality of the platform selected for the JINDEX, administrators should be able to view a management console which displays the 'up' or 'down' status of endpoint systems and web services.
T26	Depending on the native functionality of the platform selected for the JINDEX, administrators should be able to view a management console which displays the load on particular web services (e.g. number of requests in a given time period), CPU utilization of the JINDEX server(s), etc. Ideally, the console will allow the administrator to configure load alert thresholds, which, if exceeded, would allow for automated notification.

3.7 NOTIFICATION

Notification is the process of alerting the appropriate personnel or process when a business condition or rule is met. In the context of logging, the following notifications are required:

#	Technical Requirement
T27	Agency applications will be responsible to alert/notify front end users when a back-end web service is not available. If JINDEX does not provide a response, or provides an error response code, agencies must determine if and how to present this information to users.
T28	If JINDEX cannot successfully connect to an endpoint system for ID of Possible Match and CACH queries and responses, JINDEX support staff shall be notified immediately (this may be implemented in a number of manners, with email being the most likely, to be decided at design.)
T29	Alert notifications should be dispatched once and only once while the error condition exists. (For example, if the AOC system is down, the administrator should receive but a single (or limited number of) notifications, even if numerous CACH requests are received prior to the problem resolution). Once the error has resolved, either by a manual process or automatically, notifications should be dispatched again if the condition returns.

3.8 SECURITY

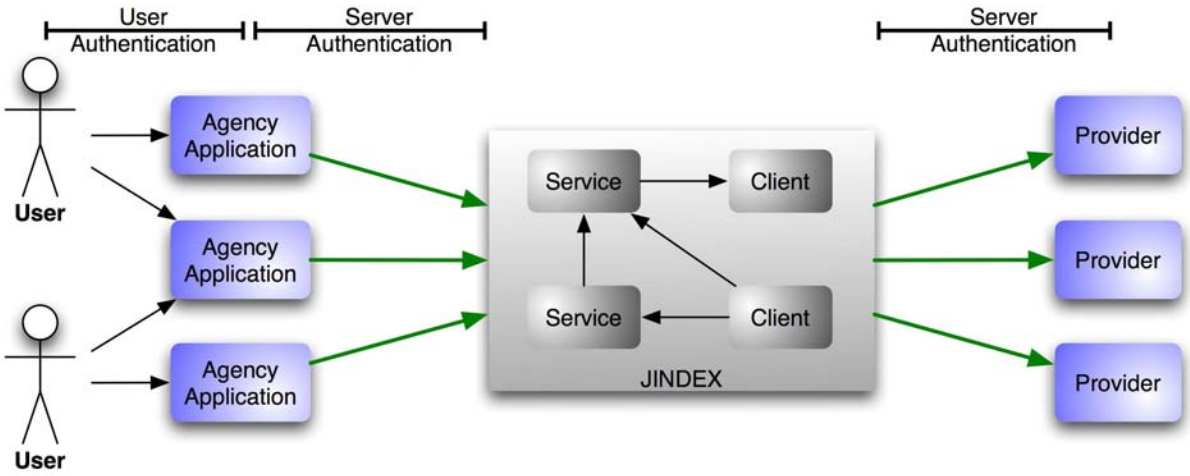
Security is thought of in terms of the following principles:

1. Privacy. Data must be shared between only authorized entities. Encryption alters the contents of messages making it difficult for third parties to decipher.
2. Authenticity. The message origins identity must allow for validation. Also, changes to the message content must be detectable. This is used to establish trust.

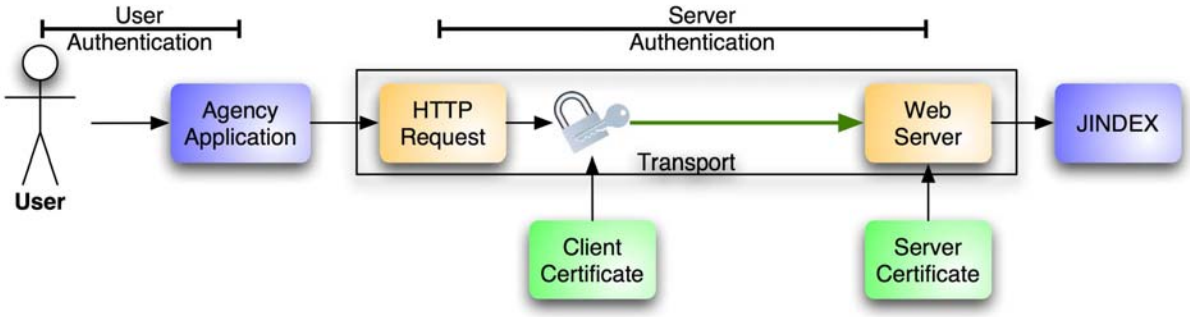
Trust and privacy will be established between the agency's application and the JINDEX, and between JINDEX and another application's services. This is to reduce the number of secured connections that must be maintained. The agency is still responsible for user authentication.

An agency does not need to maintain separate certificates for each back-end service provider – the agencies maintain only a secure contract with the JINDEX. The same is true for service providers. The JINDEX is the

only user of an external service.

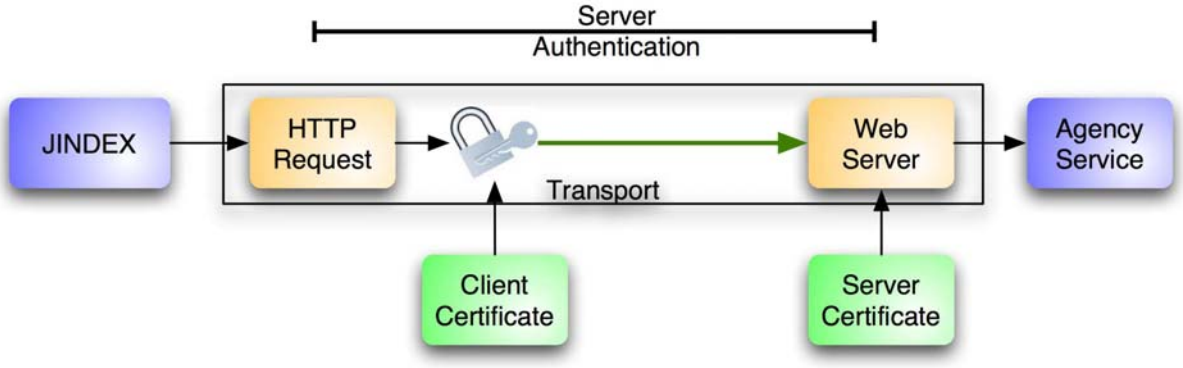


Processes using the JINDEX will require basic transport level security. Transport level security does not require application level code to work with the data as it is non-invasive. It can be changed without application changes. Secured Socket Layer (SSL) is the internet standard used to provide transport level security. SSL is commonplace in the State of Washington computing environment and is presently considered sufficient for most applications. Trust can be implemented using digital certificates.



Existing agency applications already have user authentication (whether username/password or certificate-based) and will continue to use it. Agencies are responsible for maintaining security between their system and their users. When those applications invoke services on JINDEX, then server-to-server authentication is to be used and this will be done using SSL.

Digital certificates function as a form of a signature. Agency applications can digitally 'sign' network access and then services can validate the digital signature. A key-pair will be established to establish trust. A service will sign a message in combination with the JINDEX's public key. Thus only the service and the JINDEX will be able to communicate and the information will remain private.



Transport level security can be used to meet the security requirements of existing applications. However for applications that require fine-grained security, such as message body encryption, WS-Security (WSS) is a standard that provides the semantics for securing SOAP based messages.

WSS provides message based security – meaning that the message content itself is secured. This would be required for sensitive messages where JINDEX is not a trusted resource. In traditional message broker architectures, the central broker would have visibility to the message content before delivery to the ultimate destination. If the agency requires that only the ultimate service provider be able to view the message content and not the middleware, then the agency must encrypt the message content. WSS provides the standardized semantics to SOAP based messaging. It would however be up to the ultimate consumer and the agency to negotiate the security requirements and implementation and not JINDEX.

The advantages of end-to-end message based security over transport level security may be seen once more applications, services, and users are connected through the JINDEX, since inter-agency trust may be context specific. For example, the WSP trusts King County's JILS application and has an established MOU with King County reflecting this trust. If King County adds a new publicly-accessible application, this will not fall under their existing MOU with WSP. Because, however, transport-level, server-to-server security had been implemented between the endpoints and the JINDEX, additional programming and custom mechanisms would be required to restrict the new, non-approved traffic.

#	Technical Requirement
T30	Traffic between the JINDEX and agency systems (AOC, King and Yakima counties) will be secured using server-to-server certificate-based authentication, i.e. transport level security. This is equally applicable to any agency, regardless of the network their server resides on (i.e. IGN, SGN, or Internet)
T31	Connectivity between the JINDEX and the ACCESS switch will be secured using a TCP connection over a VPN.
T32	Agencies will be responsible for acquiring their own server certificates.

3.9 NETWORK

JINDEX must support a community of users that reside on networks with varying levels of security, including the Washington State SGN, IGN, and Internet. Some applications have implemented security paradigms which grant access based on the network (predominantly SGN applications). JINDEX, however, will initially secure all CACH traffic and authenticate all servers which attempt to communicate with it, as identified in the security technical requirements.

3.10 AOC ADAPTER

The Administrative Office of the Courts hosts one of the data repositories that are essential for CACH queries, containing court, prosecution, and disposition data. The AOC hosts an IBM WebSphere application server and is currently engaging in an internal migration project, whereby legacy systems (SCOMIS, DISKUS, etc.) will be replaced with a Java-based Case Management System. As such, the AOC will implement their own 'adapter' on WebSphere, writing web service functionality using internal Java resources.

This provides an excellent example for future integrated justice projects, since:

(a) it demonstrates the technology neutrality of using web services and open standards, connecting Java (AOC) with Microsoft (JINDEX) servers, and

(b) it demonstrates how WSDL can be used in advance for service definition and integration contracts between two agencies

#	Technical Requirement
T33	The JIN CACH will provide WSDL to the AOC for the requests and the responses to the ID of Possible Match and the CACH queries. The WSDL will define implementation specifics for both SOAP headers (WS-Security and WS-Addressing), and SOAP bodies (CACH-specific Justice XML)
T34	The AOC will be responsible for any back end logic (e.g. SQL calls, stored procedures, API or method invocation, etc.) necessary to execute the web service queries once they are received by WebSphere.
T35	Because query responses will be sent asynchronously from query requests, WebSphere will need to implement a basic message store, tracking the state of completion of individual conversations. Further detail on this requirement will be conveyed in the Design Document.

3.11 WSP ADAPTER

The Washington State Patrol hosts the other system whose underlying data repositories are essential for CACH queries, containing criminal, arrest, warrant, corrections, transport, and other information.

#	Technical Requirement
T36	Connectivity with ACCESS will be achieved by establishing a TCP connection, in accordance with all requirements outlined in MSS External Interface Programmer's Guide
T37	JINDEX services will transform and translate from CACH Justice XML message formats, into the terminal syntax message formats defined in the ACCESS Manual
T38	When responses are posted from ACCESS (and hence its connected systems, such as NLETS and III) back to the JINDEX, the JINDEX will parse the character stream into the CACH Justice XML message formats.
T39	Due to performance considerations of parsing from a raw character stream (analogous to 'screen scraping') not all data from ACCESS will be transformed into XML. The entire, raw text string will, however, be provided in an appropriate XML element, such that no information is lost over what is currently provided by ACCESS.

3.12 USER INTERFACE

CACH Web Services are initially being designed for consumption by King and Yakima counties, each of which is developing internal applications that will allow for the presentation of CACH-provided data to their user communities. The JIN Program Office is also interested in how web services may be used in the future by agencies and users with varying levels of technical competency. As such, the CACH project will implement a basic user interface on top of the web services. The user interface is mainly for demonstration and testing purposes, and will not contain all of the features and functionality that are normally associated with production-ready user applications.

#	Technical Requirement
T40	CACH will implement a web page that will allow a user to input all data elements identified in technical requirement T3, for the ID of Possible Match Query. Normal web conventions shall be used for validatable or enumerated options (such as radio groups or drop downs for Sex, Race, and State, format validation for Date of Birth)
T41	CACH will implement a web page that will display all data elements contained in the results of the ID of Possible Match Query, identified in technical requirement T5. The display will contain a default sort order (to be established in the design document), but will not implement dynamic re-ordering of display results.
T42	The results page from the ID of Possible Match Query will hyperlink subject names in order to invoke the CACH Query web service. There will not be a separate web page through which to manually invoke the CACH Query web service (e.g. a page that allows for the manual entry of the various types of identifiers). Clicking on a subject name hyperlink will pass all data identified in technical requirement T6 to the CACH Query.
T43	CACH will implement a web page that will display all data elements contained in the results of the CACH Query, identified in technical requirement T8. The display will contain a default sort order (to be established in the design document), but will not implement dynamic re-ordering of display results.
T44	Because HTTP is a connection-less protocol and web service query results will be returned asynchronously, user web pages will need to be refreshed, either manually or automatically, in order to display query results.
T45	An intermediate data store may be required in order to store and collate query results for when the user refresh occurs. The data store does not need to be production quality.
T46	The user interface will not require graphic design (apart from implementation of the JIN logo)
T47	The user interface can make use of the most current version of Internet Explorer, and does not need to be designed for cross-browser or cross-version support.
T48	The user interface will not require user authentication and the associated requirement for maintenance of a username/password data store. The JIN Program Office will determine how access to the user interface will be controlled.

REQUIREMENTS TRACEABILITY

This section presents the Functional Requirements from the Customer Requirements Report deliverable and their traceability to Technical Requirements in this document. Technical Requirements are denoted as '*Tn*'.

#	Functional Requirement
FR1	**WSP ACCESS data will be accessible through an 'ID of Possible Match' query. In this query, a subset of a person's attributes is passed into ACCESS. ACCESS returns a list of persons who are possible matches based on the input.** T3, T4, T5, T9, T36, T37, T38, T39
FR2	**WSP ACCESS data will be accessible through a 'Criminal History' query. In this query, an explicit person identifier is passed into ACCESS. ACCESS returns all criminal history data for that person.** T6, T7, T8, T9, T36, T37, T38, T39
FR3	**AOC data will be accessible through an 'ID of Possible Match' query. In this query, a subset of a person's attributes is passed into AOC. AOC returns a list of persons who are possible matches based on the input.** T3, T4, T5, T9, T33, T34, T35
FR4	**AOC data will be accessible through a 'Case History' query. In this query, an explicit person identifier is passed into AOC. AOC returns all case history data for that person.** T6, T7, T8, T9, T33, T34, T35
FR5	**A 'Consolidated ID of Possible Match' query will access both AOC and WSP systems. Given a single request to the consolidated query, the query will in turn redirect the request to both AOC and WSP systems.** T3, T4, T5, T9, T12, T13
FR6	**A 'Consolidated Case and Criminal History' query will access both AOC and WSP systems. Given a single request to the consolidated query, the query will in turn redirect the request to both AOC and WSP systems.** T6, T7, T8, T9, T12, T13
FR7	**All queries will be implemented as asynchronous request/reply web services.** T12, T13, T14, T35
FR8	**JINDEX will implement reliable messaging, to include definable conversations (i.e. a CACH conversation can take different parameters from other, future conversations) and configurable parameters, including number of retries, time between retries, and escalation/notification procedures (e.g. email alerts).** T14, T15, T16, T24, T28. Note that reliable messaging will not be implemented for CACH services, as directed by the TAG. See T24 specifically.
FR9	**All requests and replies will consist of a SOAP message with an embedded Justice XML document in the SOAP body.** T9, T17, T18, T19

#	Functional Requirement
FR10	**A common JINDEX authorization service will interface with existing Washington State security gateways, injecting security tokens in the SOAP header in accordance with information received from the gateway (e.g. a user sends a basic SOAP request with no security tokens in the header. The request goes through Fortress authenticated. JINDEX authorization service builds a WSS header to inject in the SOAP header of the original message. This example is illustrative only; design will be finalized during the design phase).** T17, T18, T30. Note that the TAG and DIS have decided not to implement this Functional Requirement as originally stated. Server-to-server authentication will be implemented, and WSS' use will be limited to conveyance of username and ORI. Agencies will be responsible to build the WSS headers. See Technical Requirements cited for details.
FR11	**Standardized security tokens (e.g. username, ORI, GUID) in the SOAP header will enable external applications to perform necessary authorization, without needing to re-authenticate.** T17, T18. Similar to comments above. External applications may not use WSS headers to authorize users, but the data will be there should they choose to do so.
FR12	**AOC interaction with JINDEX will rely on GJXDM standard compliant web services which will require translation from existing repository formats into this standard SOAP/Justice XML based format. Existing interfaces may or may not include leveraging other applications that are currently interfacing with AOC.** T33, T34.
FR13	**WSP interaction with JINDEX will rely on GJXDM standard compliant web services which will require translation from existing repository formats into this standard SOAP/Justice XML based format. Existing interfaces may or may not include leveraging other applications that are currently interfacing with WSP.** T37, T38, T39.
FR14	**As an asynchronous request/reply pattern, all requests must contain the URI to which replies should be posted.** T17, T19.
FR15	**Service providers will be responsible for providing services/logic that can be accessed by a JIN common authorization service, such that, JINDEX brokers the call for authorization.** T17, T18, T30. Note that the TAG has decided not to implement this Functional Requirement as originally stated. Server-to-server authentication will be implemented. Authorization will inherently be granted based on inter-agency MOUs.
FR16	**Service calls from Agency applications will be redirected to a web service that fulfills the request embedded in the call. This is done in a location transparent fashion.** T12.
FR17	**All requests and replies will conform to the WS-I Basic Profile, and potentially other WS-I profiles, as determined in the project design phase.** This has not been separately enumerated as a Technical Requirement, but it is still applicable and will be validated/tested during implementation. Security tokens used, identified in T18, will be conformant to WS-I Basic Security Profile.
FR18	**JINDEX will be capable of validating individual messages against relevant XSD schemas (although performance considerations may recommend or dictate that validation be performed at endpoints, rather than in the messaging framework)** This has not been separately enumerated as a Technical Requirement, but it is still applicable and will

#	Functional Requirement
	be validated/tested during implementation.
FR19	**All messages sent across JINDEX will be logged. Sender, receiver, date/time, and message type will be recorded at a minimum.** T20
FR20	**Users will be able to examine JINDEX logs both for debugging and audit purposes. Access rights to examine logs will be restricted. All users will be able to examine transactions where they were either the sender or the receiver. Only selected users will be able to examine complete logs.** T20, T21, T22. Note that the statement All users will be able to examine transactions where they were either the sender or the receiver' may not be implemented. DIS will determine whether they want to support this or not, due to security considerations.
FR21	**Service status and availability will be visible to authorized users.** T25
FR22	**Service usage metrics will be visible to administrator users.** T26
FR23	**Criminal Justice Agencies / service producers (the owners of a particular service) will be able to both suspend and resume their services. Suspending a service takes it offline from the JINDEX, essentially insulating it from receiving any messages from the framework. Resuming a service brings it back online.** Support for this Functional Requirement will depend on the capabilities of the JINDEX platform, and whether or not DIS will allow external agency administrators access to a JINDEX management console.
	The JIN Program Office is responsible for the Functional Requirements below.
FR24	**JINDEX users will be able to publish standards for service development in the Center of Excellence.**
FR25	**Criminal Justice Agencies will be able to view standards for service development in the Center of Excellence.**
FR26	**JINDEX users will be able to publish code examples for service development in the Center of Excellence.**
FR27	**Criminal Justice Agencies will be able to view code examples for service development in the Center of Excellence.**
FR28	**Criminal Justice Agencies users will be able to view Service APIs for service development in the Center of Excellence.**
FR29	**JINDEX users will be able to view Service Certification Requirements.**
FR30	**Criminal Justice Agencies will be able to apply for certification of new services.**
FR31	**JINDEX users will be able to certify new services.**
FR32	**Once certified, service providers will be able to register their new services.**
FR33	**Service providers will be able to add/publish integration contracts, defining specific requirements for use of their service(s) (e.g. WSP may require the ORI security token in their SOAP header, whereas AOC may not).**
FR34	**Service consumers will be able to view integration contracts for available services.**
FR35	**Service consumers will be able to receive notification on expiry of integration contracts.**

#	Functional Requirement
FR36	**Criminal Justice Agencies will be able to register their interest in new services.**
FR37	**Service developers will have a platform upon which new services can be developed.**
FR38	**Service developers will have a platform upon which new services can be tested.**
FR39	**Criminal Justice Agencies will be able to access central consolidated web services.**

APPENDIX A – GLOSSARY OF TERMS

Several terms and acronyms are used throughout this document and are briefly explained here:

JIN – Justice Information Network. The overall Washington State Program for integrated justice.

JINDEX – The JIN Data Exchange. This includes the integration broker, the technical infrastructure for implementation, common services and the Center of Excellence for future development projects.

CACH – Case and Criminal History. While this project was initially named *Criminal History Query,* stakeholder feedback has indicated the important distinction between case and criminal history information. As such, CHQ is relabeled CACH (Case and Criminal History).

Web Service – A software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a format that machines can process (specifically WSDL). Other systems interact with the Web service in a manner prescribed by its description using SOAP messages, typically conveyed using HTTP with XML serialization in conjunction with other Web-related standards (W3C).

A programmatic interface to a capability that is in conformance with WSnn protocols

Service-Oriented Architecture SOA – The policies, practices, frameworks that enable application functionality to be provided and consumed as sets of services published at a granularity relevant to the service consumer. Services can be invoked, published and discovered, and are abstracted away from the implementation using a single, standards-based form of interface.

SOA as a style resulting from the use of particular policies, practices and frameworks that deliver services that conform to certain norms. Examples include certain granularity, independence from the implementation, and standards compliance. What these definitions highlight is that any form of service can be exposed with a Web services interface. However higher order qualities such as reusability and independence from implementation, will only be achieved by employing some science in a design and building process that is explicitly directed at incremental objectives beyond the basic interoperability enabled by use of Web services.

MESSAGE – As defined by the WS-I standards adopted by JINDEX. Protocol elements that transport the ENVELOPE (e.g., SOAP/HTTP messages).

ENVELOPE – The serialization of the soap:Envelope element and its content.

DESCRIPTION – descriptions of types, messages, interfaces and their concrete protocol and data format bindings, and the network access points associated with Web Services (e.g., WSDL descriptions).

INSTANCE – Software that implements a wsdl:port or a uddi:bindingTemplate.

CONSUMER – Software that invokes an INSTANCE.

SENDER – Software that generates a message according to the protocol(s) associated with it.

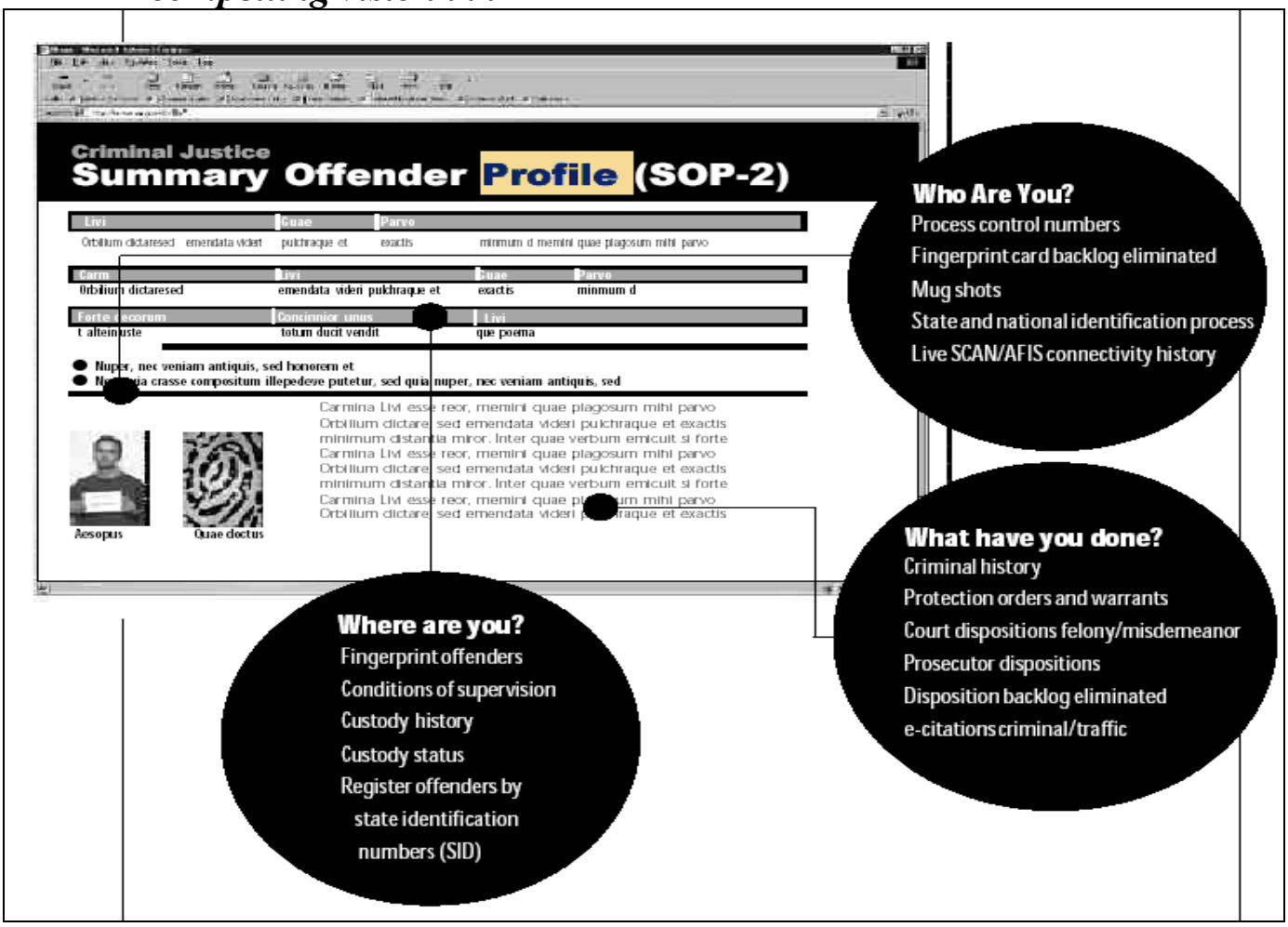
RECEIVER – Software that consumers a message according to the protocol(s) associated with it.

REGDATA – Registry elements that are involved in the registration and discovery of Web Services (e.g. UDDI tModels)

ATTACHMENT B

Summary Offender Profile: Lessons for the JIN Community

A compelling vision . . .



The Summary Offender Profile initiative (SOP) has been the cornerstone of the state's integration efforts for over ten years. In 1993, the *Justice Information Strategic Plan* described the vision for consolidated justice information in this way:

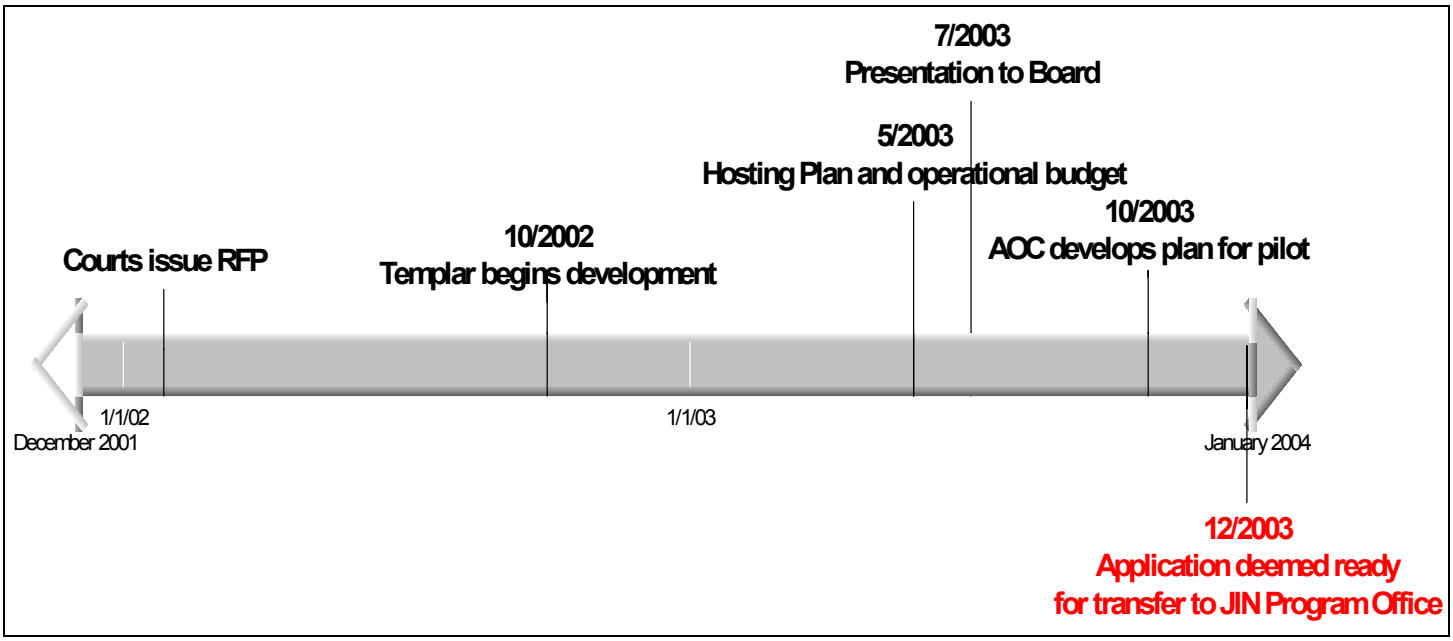
> Any justice practitioner in the state will have complete, timely and accurate information about any suspect or offender. This information will include criminal history and current justice status, will come from data that has been entered only once, and will be available in a single computer session.[1]

---

[1] *Justice Information Strategic Plan, 93-95 update, p. 3*

The 1999-2001 Justice Information Network (JIN) Blueprint further anticipated justice integration efforts as providing "a single source of information necessary to make daily decisions on criminal cases as they are processed through the stages of the justice system."[2] In 2002, the SOP was specifically envisioned as a 'one-stop shopping center' for essential information to facilitate the movement of an offender's case through critical stages of the justice system."[3]

Using $600,000 of grant funds, the AOC volunteered in 2002 to manage the project on behalf of the JIN community. In early 2004 the application was deemed ready for production and handed over to the JIN Program Office, created in April 2003, which had developed a bare-bones support plan, funded by $100,000 of Byrne Grant funding from OFM. Once the servers had been installed in the DIS data center and the application was up and running, the JIN Program Office commenced a pilot deployment, which had originally been slated to be run by AOC in the test environment.



The pilot revealed that, although it showed promise, the application did not immediately demonstrate a business utility and that additional user documentation and training would be required.

Since that time, the JIN Program Office has continued to seek out possible users for the application, and some corrections and law enforcement officers have expressed interest. The Program Office has also begun plans for an XML-based Court and Criminal History Query that will leverage much of the work done for SOP.

---

[2] 1999-2001 Biennial Integration Blueprint (http://www.jin.wa.gov/publications/jinbluprint.pdf).
[3] JIN Project Status Report, August 2002 (http://www.jin.wa.gov/meetings/2002/091702sopStatusreport.doc).

Summary Offender Profile: Project Assessment

What went right	Reason	Lessons Learned	Subsequent Action
Created web-based interface to aggregate WSP ACCESS and AOC data.	►State systems are robust and usable. ►Cooperation of stakeholder agencies	Project goals are achievable without changes to existing systems.	CACH will use this work.
Created operational support model in JIN Program Office.	Subsidized by Byrne Grant funds from OFM.	►Outsourced support model is difficult but feasible. ►Managing services and products requires resources.	JINDEX servers to be hosted in DIS dedicated environment.
Created workable security model for access to application throughout the justice community.	Driven by WSP rules.	Existing policies should drive requirements for new applications.	CACH will use this work.
What went wrong	**Reason**	**Lessons Learned**	**Subsequent Action**
JIN Program Director did not fully understand the state environment.	Hired from outside, April 2003	►Listen to the community. ►Don't rush. ►Don't believe the hype.	►Created Technical Advisory Group ►Developed understanding of user community and began to build relationships with key stakeholders.
Insufficient requirements gathering.	►Project sponsor (JIN Community) had no dedicated resources. ►Managing agency (AOC) did not see itself as an end-user.	Future services should be driven by user demand.	►Principle incorporated into *2005 Blueprint* (p.20) ►"JIN" projects limited to those managed by the JIN Program Office (*2005 Blueprint*, Appendix G).
Proprietary solution limits extensibility options	►Standards like Justice XML and web services were not mature at project commencement.	Future solutions should be open and standards-based.	*JIN Technology Principle* #1.

	►No JIN Technology and Design Principles.		
One application cannot be all things to all users.	Lack of involvement of end-user community in requirements gathering. Overly ambitious.	Services should be more flexible and adaptable.	Use Justice XML and web services for CACH, future JINDEX services..
Developer was not a user.	►No-one else volunteered. ►Project commencement predated JIN Program Office.	Need end user as champion.	King and Yakima County are key partners and will be used to develop requirements for and validate CACH service.
JIN community did not assume ownership	►No infrastructure. ►Differing interests. ►Lack of resources.	Need empowered and funded Program Office to manage projects on behalf of the Board.	2005 Decision Package adds resources to Program Office.
Difficult to work with developer located in Virginia.	►Time difference. ►Limited face-to-face interaction.	Geography and availability are important.	JINDEX project team is Portland-based.
Pilot not completed before application certified as ready for deploymen.t	Pilot was not part of initial plan Changing environment at AOC.	Make sure application is ready and field-tested before deployment.	►Full functional testing to be completed for JIN CHQ CACH. ►King and Yakima county users to serve as testing ground.
Insufficient user documentation.	►Overly ambitious expectations regarding ease-of-use. ►Lack of resources.	Need dedicated resources to manage JIN projects.	►JIN Program Office created April 2003. ►JIN Budget Request 2005-07 biennium.

ATTACHMENT C

E-TRIP INFRASTRUCTURE
STATEMENT OF WORK (March 7, 2005 DRAFT 2.1)

1.0 PURPOSE

The Department of Information Services (DIS) on behalf of the Washington Integrated Justice Information Board for the state of Washington seeks to engage Contractor for the purpose of designing the model for E-Trip data exchanges and constructing an interface for the exchange of electronic traffic records information. The State is seeking solutions based on an open, standards and service-based architecture that uses the Justice Information Network Data Exchange (JINDEX) and improves the flow of information in a flexible and cost-effective manner. The State seeks solutions that correspond to the Justice Information Network (JIN) design and technology principles (http://www.jin.wa.gov/standards/index.htm).

2.0 WORK

The Contractor shall provide the services and staff, and otherwise do all things necessary for or incidental to the performance of the Work as set forth below. Contractor shall propose a plan that sets out clear milestones and deliverables on a monthly basis, which facilitates breaking the project up into manageable and logical components. Contractor shall submit all deliverables to the E-TRIP Steering Committee for review and approval or if the document is not approved, modification and resubmission for review and approval. Any additional services provided by the Contractor must have prior written approval by DIS. DIS reserves the right, at its sole discretion, to cancel or eliminate any phase or any deliverable specified in a particular phase prior to performance thereof by giving written notice to Contractor, and neither DIS, the Board nor the State shall incur any liability for such action.

The Contractor shall, as further described in this statement of work, perform the following:

1) Examine and design the architecture for the exchange of electronic citations and collision report data based on customer requirements and current operational environments. To aid in this process, the following documentation is included: Contractor shall model the current data exchanges and propose an architecture that makes optimal use of JINDEX, which will use Microsoft BizTalk as its integration platform and facilitate data exchanges in the justice community using web services and Justice XML. The Contractor shall also recommend modifications or enhancements to JINDEX, including governance issues, necessary to support the E-TRIP exchanges.
2) Design and develop, based on the State Citation and Collision Forms (Attachments A, B and C) a set of XML-enabled forms or processes that will allow LEAs and local entities to input and transmit citation and collision data in a manner consistent with the process described herein. This work will include XML schemas for the exchanges that make optimal use of the NCSC Functional Requirement Standards for Traffic Case Management Systems, the Global Justice Data Exchange Model and Data Dictionary (GJXDM and GJXDD), AAMVA standards and DHIP requirements
3) Develop, test and deploy a set of interfaces and messaging transactions that allows citations information to be electronically exchanged among the Law Enforcement Support Agency (LESA), Pierce County District and Tacoma Municipal Courts, the Administrative Office of the Courts (AOC) and the Department of Licensing

(DOL), in conformance with all business requirements. These transactions will make optimal use of web services and the JINDEX.

Contractor shall perform the services and provide the key deliverables further described in this SOW in the estimated timeframes established below:

- Project Award May, 2005
- Design June 2005
- Develop Exchanges July 2005
- Implement September 2005

3.0 APPROACH

Contractor shall propose a methodology and approach by which work will be delivered. Contractor's proposed approach should clearly identify all phases, milestones, and deliverables that Contractor proposes. As a guideline, the State desires an approach that includes milestones and/or deliverables at intervals of no more than one (1) month.

The State forsees at a minimum the following groupings of activities and associated deliverables. Contractor shall clearly describe the intent and content of all proposed deliverables.

3.1 Design

Contractor shall perform facilitated sessions and interviews of E-TRIP constituents to identify customer requirements (functional and non-functional), including those not provided by the current JINDEX architecture.

Contractor shall document all assets and system capabilities, such as the current operational environment; existing automated and manual processes; opportunities to improve operations through the use of IT; overriding business and service delivery objectives; constraints and legal mandates; data sharing or exchange processes; current and impending system requirements; inventory of existing information systems used by the stakeholder organizations; and internal and external factors that will influence system direction.

Contractor shall create a high level design for information sharing and connectivity that addresses all identified requirements and makes optimum use of reusable components through JINDEX.

The design will provide sufficient detail to enable the State to understand the changes that will be required to the current environment (including JINDEX) and the manner in which system components will interact. The design will provide sufficient detail to enable all E-TRIP constituents to identify opportunities to change their existing business practices to increase efficiency and effectiveness.

Deliverable: Design Document

3.2 Development

3.2.1 DEVELOPMENT OF XML SCHEMAS

To accompany the design, Contractor shall prepare a set of XML schemas for citation and collision exchanges among AOC, DOL, WSP, WSDOT and LESA. These schemas will be compliant with GJXDM, GJXDD and the reference documents mentioned herein.

Contractor shall provide the schemas to the JIN Project Manager for review and any necessary updates, based on communications with the data sources or users.

Deliverable: XML Schemas

3.2.2 DEVELOPMENT OF XML-ENABLED FORMS

Using the schemas developed in 2.2.1, Contractor shall prepare a set of XML-enabled forms, based on the state models for citations and collisions. These forms will be made available through the JIN Program Office for use by the E-TRIP community.

Contractor shall submit the draft report to the JIN Project Manager for review and approval or modification. Upon approval, the Contractor shall then present the report to the E-TRIP Steering Committee for review and approval, or if it is not approved, for modification and resubmission.

Deliverable Citation Form
Infraction forms
Collision Form

3.3 **Development And Installation Of Data Exchange**

Using the agreed-upon design Contractor shall develop working services to facilitate the exchange of data from [LEA] with AOC and the transmission of data from AOC to DOL using the JINDEX and the standards and principles mentioned herein. Contractor will also develop a test plan to validate the transactions and complete functional testing to confirm that the process is fully operational.

This task includes the development of all objects required to build the Web Service; the conducting of user interface testing; and any necessary training.

Contractor shall deliver a fully operational service, including the following:

- Full design and development documentation
- All source code, including code for the services
- Functional testing and validation
- Operational, hardware/software cost estimates
- Test suite for validation of future modifications

Contractor shall provide the deliverable and all documentation to the JIN Project Manager for review and any necessary updates. Upon approval, the Contractor shall present the deliverable and documentation, including any updates, to the E-TRIP Steering Committee for review and approval or if the deliverable is not approved, modification and resubmission for review and approval.

Deliverable: Construction, validation and implementation of LEA ► AOC ►DOL e-citations services

4.0 PROJECT SCHEDULE

The Contractor shall provide a project schedule to the DIS Project Manager within five days of the execution of the contract. The project schedule will include all of the deliverables identified in this Statement of Work, but may propose additional deliverables and need not follow the order presented herein. Additional deliverables must be specified in the executed contract. The Contractor shall revise the project schedule upon request of DIS.

5.0 DELIVERABLES AND REPORTS

Contractor shall work with the JIN Project Manager to establish deliverable review and approval processes, including methods for reviewing interim deliverables and presenting final deliverables. Deliverables shall be provided in hard copy and electronic file in Microsoft Word® and Adobe Acrobat® formats. Presentations shall be provided in Microsoft PowerPoint®. The Contractor must provide source data files for special deliverables (e.g. graphics, tables or other exhibits created for this contract); and special software, documentations, and instructions required to enable the State of Washington to update and publish revisions to the plan.

Contractor shall provide at a minimum the following deliverables and reports:

a) Contractor shall produce each and every deliverable identified in this Contract.
b) Contractor shall provide monthly progress reports to the DIS Project Manager including the list of any deliverables or progress made to complete the deliverables, recent activities, changes to the current schedule, issues and action plans.
c) Any other reports requested by DIS.

~~d)~~

6.0 LOCATION OF WORK

Although most of the work can be done offsite, the State expects the Contractor will spend several days with the project team onsite in Washington State at the beginning of the project. The Contractor will also be expected to attend required meetings and to be in Washington State to facilitate the review of reports created by Contractor.

Contractor shall be available in Olympia, Washington to the DIS Project Manager via telephone and email and for scheduled work events, meetings, presentations and conferences during regular business hours from 8:00 am to 5:00 pm, Pacific time, Monday through Friday.

Contractor shall provide their own personal computers, software, email and communication accommodations.

Contractor shall make their own travel arrangements and shall pay for their own travel expenses.

Contractor shall use their own office locations in order to complete work products outside of scheduled meeting events.

7.0 CONTRACTOR PERSONNEL

If at Contract award or any time thereafter, any specifically named individuals identified in the Contractor's Response to the RFP are not available, DIS has the right to approve or reject any change in Contractor personnel.

ATTACHMENT D

Justice Information Network (JIN) Decision Package
Applicant: Justice Information Network Program Office
Decision Package Title: JINDEX Services

Budget Period: October 2005-August 2006

Recommendation Summary Text:

In 2005, the JIN Program Office began the implementation of an integration platform to permit information sharing in the justice community. This platform, known as the JIN Data Exchange (JINDEX) uses the principles of service-oriented architecture (SOA) to achieve maximum efficiency without imposing fiscal or technology mandates on state and local constituents. This decision package envisions the addition of key services to the JINDEX architecture in a manner that will optimize benefits and flexibility for the community. In keeping with the JINDEX model, the services proposed herein may be considered as standalone components. They are submitted together purely for reasons of logic and convenience, and to reduce the overall cost of establishing a test environment, which will allow for the validation of new JINDEX services before deployment.

Narrative Justification and Impact Statement

The JINDEX will provide a foundation for future justice information sharing initiatives within the State enterprise and among local government entities—a statewide plan and technology infrastructure for securely and reliably sharing information amongst the JIN community. The JINDEX will deliver an integration technology foundation based on the principles of a service-oriented architecture (SOA). The JINDEX provides a solution that makes optimal use of existing infrastructure and with the smallest possible impact on existing systems.

The JINDEX builds on the steps taken by the state to establish a framework and strategy for integrated justice, beginning with the creation of the Washington integrated Justice Information Board (the Board) and the JIN Program Office in 2003, and the subsequent report of the Board to Governor Locke in September 2004 (http://www.jin.wa.gov/publications/strategicplan2005.htm.) This process was further supported by the state's decision to provide Byrne grant funding for the creation of JINDEX in 2004. This led to the engagement of contractor assistance at the end of 2004; the selection of Microsoft BizTalk as the technology platform in early 2005 and the design an implementation, in partnership with King and Yakima County of web services to provide seamless interface with the state repositories of criminal history and court information (the "Court and Criminal History (CACH) query, scheduled for completion in June 2005). The Customer Requirements and Baseline Requirements Report for this project are included with this package as Appendices A and B.

This decision package proposes the creation of a development area in the JINDEX to allow services to be tested and validated before deployment; the creation of an XML-enabled incident report in collaboration with the Law Enforcement Support Agency; collaboration with King County and DIS on a study of the feasibility of a web services interface for the DOL's Driver and Plate Search; and the expansion of the CACH web service to include DOL photos and additional queries available through the state ACCESS switch.

How the Decision Package contributes to the applicant's strategic plan
The 2005 JIN Blueprint identifies four key strategies for integrated Justice in Washington":

1. Design the Justice Information Network
2. Develop technology and design principles
3. Develop services in response to user demand
4. Maintain security and privacy rights

The JINDEX provides the architecture for the physical and logical flow of information in the justice community—the infrastructure and business rules for the exchange of information and the foundation for future services beyond the CACH Query. This decision package proposes services identified by the justice community as ideal candidates for the JINDEX.

How the Decision Package supports the JIN Mission and Objectives
This Decision Package supports the JIN mission and objectives by using standardized data and communications protocols (Justice XML, web services) and existing infrastructure (JINDEX) to deliver more complete, timely and accurate information to the justice community, and to do so in a way that allows other users to derive maximum benefit from services constructed for initial use by specific jurisdictions.

How the Decision Package aligns with applicable grant requirements or objectives
For Byrne, each component of the decision package represents a direct and tangible improvement in the exchange and availability of criminal history records, improving the operational effectiveness of law enforcement (2004 purpose area #7).

For NCHIP, the proposal will improve the state's Records Quality Index by improving the automation of records and providing local jurisdictions more complete access to state files, particularly the WSP and DOL. The proposal also supports Priority 1 by improving access to protection orders; and Priority 6 by providing more complete records in a standards-based manner that facilitates sharing and interoperability.

How the Decision Package aligns with the JIN Technology and Design Principles:
The technology and design principles were the standards set to facilitate and guide the design and development of JINDEX. The JINDEX builds on these principles by using shared infrastructure (DIS, AOC, WSP), national standards (SOA, web services, Justice XML) and reusable components to facilitate exchanges in conformity with existing security and privacy requirements in a way that allows data providers to retain full control over who has access to their information.

Resources Required
In addition to the service of the JIN Program director and staff (if funded), the project will rely on the continued administrative, legal and technical support of DIS for staffing, equipment and facilities.

Revisions required in an existing statute, Washington Administrative Code (WAC), contract, or state plan in order to implement the change.
None

A distinction between one-time and ongoing functions and costs.
The implementation of a development area for JIN is a one-time cost that will facilitate the building and testing of future services. The services to be developed will use consultant resources, and future upgrades can be provided by the JIN Program Office (depending on the complexity of the change and assuming the funding of this year's budget request, which adds a technical staff person). The implementation of the services proposed can be achieved in the environment created by the JINDEX and, although the operating environment for JIN constituents will be dramatically improved, the new services will not impose significant additional operating costs on the JIN Program office. Match requirements will come from the contributions of JIN staff and connectivity costs in the DIS Dedicated Environment, the operational home of the JINDEX hardware.

Fiscal Detail

Hardware and software for development environment 2 servers (Biz Talk, SQL)($15,000) MSDN License $1,200 Other Software ($3,800)	**$20,000**
Consultant assistance on the feasibility and design of a web service interface for DAPS in collaboration with DIS and King County	**$25,000**
Consultant assistance on the development of an XML version of the incident report in collaboration with LESA	**$50,000**
Consultant assistance on the development, design and deployment of a service adding DOL photos to JINDEX (may be some hardware/software required)	**$100,000**
Consultant assistance on the development of web services components for specific ACCESS queries in collaboration with King and Yakima Counties.*	**$155,000**
TOTAL	**$350,000**

Attachment A: Project Management Plan and Schedule

It is envisioned that each component can be completed in a period of approximately 4-8 weeks, and that a single request for proposals can be used to fund all activity in this package, with projects to be opened and closed incrementally—maintaining the option to modify or terminate the vendor-client relationship at the completion of any phase. The JIN Program Director will manage the project and engage an appropriate subset of Technical Advisory Group members for service on a steering committee to review proposals and provide project governance. The JIN Program Director will provide periodic reports to the Board, which, by design, is available to resolve high-level policy issues.

It is envisioned that the project can proceed roughly in accordance with the following schedule:

Assemble Steering Committee	August 2005
Issue RFP	October 2005
Contract Award	December 2005
Design and deployment of development environment at DIS	January 2006
Design and deployment of granular ACCESS services for JINDEX	February 2006
Testing and deployment	March 2006
Design and deployment of XML Incident report	April 2006
Testing and deployment	April 2006
Design and deployment of web service for addition of DOL photos to JINDEX	May 2006
Testing and deployment	June 2006
Feasibility study of DAPS web service	July 2006

PROJECT ORGANIZATION

ROLES AND RESPONSIBILITIES

Role	Assigned to	Project Responsibilities
Project manager	JIN Program Director	1. Project management and leadership 2. Communications and management of expectations
Manage Operational Environment	DIS JIN Technical staff	1. Business area expertise 2. Technical expertise 3. Assess feasibility of how services will be delivered and developed
Steering Committee	Technical Advisory Group	1. Ensure project goals and objectives are met 2. Decisions on changes in project scope 3. Resolve issues escalated by project managers or other project team(s) 4. Elevate major policy issues to Board
Executive Sponsor	Justice Information Board	1. Policy oversight and direction 2. Resolve issues as needed

PROJECT INFORMATION

Add ACCESS Queries to JINDEX

The CACH Query will make court and criminal history information available through the JINDEX using XML and web services. In addition to criminal history, there are approximately two hundred queries available through ACCESS (See Appendix C). Although the Technical Advisory Group (TAG) identified criminal history as paramount, items like warrants, the Interstate Identification Index (III), protection orders, etc. are also crucial to the optimum exchange of information in the justice community.

This proposal envisions asking the TAG to prioritize the queries and then using consulting assistance to make them available through the JINDEX using the security and performance model developed for CACH.

XML Incident Report

The Law Enforcement Support Agency (LESA) has begun work on the creation of an XML version of its incident report (see Appendix D), but this includes only 20 data elements of the several hundred available and described by the GJXDM. This proposal aims to engage consultant assistance to create a complete version of the incident report and to make it available to all law enforcement agencies in the state through the JIN Program Office. This will involve creating a statewide XML schema for data to be included in the report, as well as a state template and a customized LESA report for deployment in the field.

Design and deployment of web service for addition of DOL photos to JINDEX

JINDEX will create the integration platform for the exchange of information in the justice community. It is clear from discussions with state and local law enforcement, that on-line access to DOL photos would be an extremely valuable tool in helping officers confirm that the person in front of them is who he or she claims to be.

Although DOL has approved this proposal in theory, there are many steps in developing and implementing an acceptable model for making this happen. This proposal envisions using a model similar to that employed for the JINDEX to use a collaborative model for gathering customer requirements (performance, security, etc); developing and validating a design document; and implementing a web service to allow JIN constituents to access the information.

Feasibility study of Driver and Plate Search web service

The DOL Driver and Plate Search (DAPS) (http://www.dol.wa.gov/vs/daps/daps_manual_version5.1.pdf) is a web-based search tool. for locating a vehicle or driver record when only partial information is available. Conversations with local entities suggest that a web services interface would help to increase the level of adoption of the new service and also increase its utility, by allowing users to run DAPS queries within their local applications.

Conversations with DIS and the JINDEX project team suggest that the current configuration of the JINDEX and Transact Washington (the authentication method for DAPS) would not support a web service interface to DAPS through the JINDEX, but also that there are potential technical solutions. This proposal envisions using consultant assistance to work with DIS, DOL and the JIN community to determine the feasibility of the proposal and the associated level of effort with developing a web services interface for DAPS and making it available through JINDEX.

Budget Period: November 2005 – July 2006

Recommendation Summary Text:

King County plans to incorporate the ability for law enforcement officers to inquiry wants and warrants within the County's Justice Information Look-up Service (JILS). JILS is a secured web-based application that allows every law enforcement officer in King County – both from the King County Sheriff's Office and all other municipal police agencies – to obtain certain information from any location with Internet access, including wireless roaming PCs. Under this proposed project, warrant information and "person of interest" alerts would be included as information available in JILS.

This project involves the development effort required to incorporate wants and warrants information within the existing JILS application. It is dependent upon the state JIN project developing a "Web Services" capability to request and receive such information.

Fiscal Detail

The budgeted cost of the King County project is $520,000, with $187,173 directly associated with the design and development work required to connect to a JIN-hosted Web Service. The line item detail for this budget is as follows:

Line Item	Budget
Project Salaries, Wages, Benefits	$61,845
Supplies, Telecom, Printing	$5,200
Technology Development Services*	$421,564
*Portion associated with connection to JIN Web Service	$187,173
IT Internal Services (maintenance)	$31,200
Total	$519,809

The funds associated with this project have been appropriated and committed by the King County Council for the LSJ Integration Program.

Narrative Justification and Impact Statement

King County Program Background

In 2002, King County adopted a Law, Safety and Justice Strategic Integration Plan. This plan identified business activities within the criminal justice operations of King County that could be improved through technology integration, defined specific projects intended to improve those operations, and established the LSJ Integration Program within the County.

The mission of the King County LSJ-I Program is to improve the efficiency and management of criminal justice cases, and improve the safety of King County citizens, through the effective and timely sharing of criminal justice information with decision makers and law enforcement officers.

Project Information

Within the funded scope of the LSJ-I Program, the County identified the improved ability to identify warrants as one of the top operational priorities, and defined "Improved Warrant Management" as one of the six funded sub-projects within the LSJ-I Program. This project seeks to address the following operational challenges:

1) Presently, field-based law enforcement officers do not have direct access to criminal warrants. Most agencies establish policies limiting the situations in which an officer would request warrant information during field situations, due to the burden on radio communications to request such information. King County wishes to create the ability to perform inquiries to criminal justice information using a web-based application that could be accessed from any PC by a user with proper authentication.

2) When an inmate is booked into a King County jail facility, the county checks for warrants. Jail staff does so again at the time an individual is released from jail to ensure valid release status. However, the county makes no such check of warrants during the detention of an individual. King County wishes to create an automated method to check for new warrants issued for current inmates on a regular basis, for the purposes of improving inter-agency communications and expediting criminal proceedings.

This project would improve the ability for law enforcement officers throughout King County to obtain information on wants and warrants. This supports the objectives of using technology to inform law enforcement officers of potentially dangerous individuals, including individuals involved in domestic violence. It would provide information to decision makers in a real-time, inquiry-based manner, delivering complete, accurate, and timely information immediately when required.

Project Alignment to JIN

King County will accomplish this project by leveraging a Web Service delivered by the Washington State Justice Information Network (JIN). The JIN service would accept an inquiry about an individual and return wants and warrants information. At all times, the exchange of information would be secured through user authentication and encrypted communications, and would comply with standards regarding data exchanges.

As proposed, this project is consistent with the objectives of the JIN. As the largest criminal justice jurisdiction in Washington State, the adoption of JIN services in King County will provide the leadership necessary to ensure success of the overall JIN program. This project directly aligns to the technical blueprint of JIN by leveraging the planned service oriented architecture, and supports the business strategy of JIN by realizing the mission of the program – "improve public safety by providing criminal justice practitioners with complete, timely and accurate information."

Project Alignment to NCHIP

This project aligns to the NCHIP program priority for "strengthening records to improve national security standards and avert terrorism." By providing the tools necessary for field-based inquiry of information regarding persons of interest, law enforcement officers will have the ability to knowledgably interact with individuals and make appropriate decisions regarding potential detention of such individuals.

Within this priority, this project further meets the following review criteria as outlined for the NCHIP program:

- Support/enhance participation in the NCIS, III, the National Sex Offender Registry, the NCIC Protection Order File, the National Crime Prevention and Privacy Compact, and other related Federal and State systems: This project extends access to State and Federal warrant repositories to field-based law enforcement officers.

- The proposed use or enhancement of innovative procedures which may be of value to other jurisdictions: The results of this project will be available to law enforcement agencies outside the King County Sheriff's Office.

- The technical feasibility of the proposal and the extent to which the proposal appears reasonable in light of the State's current level of system development and statutory framework: This project leverages an existing end-user system, and builds upon the JIN pilot project.

- Reasonableness of budget: The budget for this project is based on other similar projects in King County.

- Nature of the proposed expenditures: The expenditures to be funded under this application are those directly related to technology development required to connect and interact with the state services.

- The reasonableness of the relationship between the proposed activities and the current status of the State system, in terms of technical development, legislation, current fiscal demands, and future operating costs: This project is in direct alignment to – and partnership with – the State's JIN Program.

Project Cost Alignment to NCHIP

King County requests $187,173 for this project, which is the portion of the overall project costs directly associated with design and development of the Web Service interface between King County and Washington State. The expenses for this project align to the following "allowable costs" for NCHIP:

- Interface between criminal history records, sex offender registry, and civil protection order files: Some of these records are also presented in JILS, thus allowing law enforcement to access these multiple records in a single inquiry.

- Reducing cost of criminal record checks: Proposed operations would streamline the criminal record checking process for law enforcement officers.

Attachment A: Project Management Plan and Schedule

In the performance of technology projects, King County deploys a standard system development lifecycle methodology with five phases. Projects report to a Project Review Board, which monitors monthly progress, controls funding releases, and retains the authority to audit and/or suspend troubled projects.

Based on current planning assumptions for the LSJ-I Program and the Improved Warrant Management Project, the high-level project plan with scheduled milestones for this project is as follows:

Washington State Web Service technical design .....November 30, 2005
Develop King County operational requirements .....November 30, 2005
Design King County technical solution.....January 15, 2006
Plan King County implementation and testing .....January 30, 2006
Washington State Web Service development.....March 30, 2006
Develop JILS v3.0 enhancements .....March 30, 2006
Complete technical testing.....April 31, 2006
Implement technical and operational changes.....May 15, 2006
Perform post-implementation operational assessment.....July 31, 2006

Since King County is greatly dependent on the delivery milestones of the state's associated JIN project, these dates assume a state project start of October 1, 2005, and make other assumptions regarding the scope or work planned by the state. These dates may be impacted by changes or differences in the state project schedule.

Justice Information Network (JIN) Decision Package
Applicant: **Washington State Patrol**
Decision Package Title: **Live-Scan Interfaces, Replacements, and Acquisitons**

Budget Period: July 2005 – September 2006

Recommendation Summary Text:

The Washington State Patrol (WSP) recommends $896,000 be used to 1) interface existing Cross Match live-scans at sites with the Spillman records management system (RMS); 2) replace older live-scan devices facing end-of-life; and 3) acquire additional live-scan systems to further reduce paper fingerprint card submissions.

1) The request to interface existing Cross Match/Spillman RMS sites will provide workload relief to local law enforcement agencies and correctional facilities. The same data are entered into each system – an interface will eliminate this redundancy, improve timeliness, and reduce the opportunity for data entry errors. The Cross Match live-scan vendor has offered a reduced cost to develop and implement this software interface. There will be no costs charged by Spillman.

2) The request is to replace older live-scan systems will provide continuation and possible upgrade of current functionality and services. The operating system on these live-scan devices is facing end-of-life and will no longer be supported by the vendor, repair will be on a time and materials basis, and the devices cannot be upgraded with peripheral options, such as capturing palm prints and establishing a records management system interface. The agencies may not be able to afford the time and materials maintenance contract and if the live-scan system cannot be repaired or replaced with local funding, the agency will no longer be able to electronically submit criminal fingerprints, there will be no real-time identification, and the criminal history record will not be updated immediately. WSP staff will have to convert the paper fingerprint card submissions to an electronic format before they can be processed and transmitted to the FBI.

3) The request to acquire additional live-scan systems for municipal jails will further reduce the paper submissions of criminal fingerprint cards. Approximately 80% of all criminal submissions are electronic and the majority of the remaining 20% submissions are coming from sites without a live-scan device. From November 28, 2004, through January 15, 2005, WSP staff tracked the incoming paper fingerprint arrest cards to determine the booking agencies with 5% or higher of the total current paper submissions.

Fiscal Detail

The total cost of the live-scan interfaces, replacements, and acquisitions is $896,000. The item detail for these costs is as follows:

Line Item	Cost
Live-Scan/RMS Software Interfaces	$56,000
Live-Scan End-of-Life Replacements	$690,000
Live-Scan Acquisitions	$150,000
Total	$896,000

1) To interface existing Cross Match live-scans at sites with the Spillman records management system (RMS) will cost $4000.00 per device.

There are fourteen (14) Cross Match/Spillman sites:

Aberdeen PD
Adams County Jail
Asotin County Jail
Columbia County Jail
Ferry County Jail
Garfield County Jail
Grays Harbor Jail
Island County Jail
Klickitat County Jail
Lincoln County Jail
Pacific County Jail
Pend Oreille County Jail
San Juan County Jail
Skamania County Jail

Operating Expenditures	**YEAR 1**	**YEAR 2**	**Total**
Software Interfaces	$56,000	0	$56,000

2) There are twenty-three (23) sites with older live-scan devices facing end-of-life. Eighteen (18) of these sites have current live-scan/RMS interfaces. Replacement is estimated to cost $30,000 per device.

The following priority is listed by the percentage of criminal history record (CHRI) submitted to the WSP:

CHRI %	Agency	Live-Scan Device	RMS	Interface
7	Spokane Jail	Identix	PRC	
4	Clark Jail	Visionics	Local	Y
4	Yakima Jail	Identix	Spillman	Y
3	Chelan Jail	Visionics	Spillman	Y
3	Cowlitz Jail	Identix	JAMS	Y
3	Kitsap Jail	Visionics	Local	Y
3	Thurston Jail	Identix	ATIMS	Y

2	Benton Jail	Visionics	BiPin	Y
2	Franklin Jail	Visionics	BiPin	Y
2	Lewis Jail	Identix	Spillman	Y
2	Skagit Jail	Identix	Spillman	Y
2	Whatcom Jail	Visionics	AS400	Y
1	Clallam Jail	Identix	AEGIS	Y
1	Grant Jail	Identix	Spillman	Y
1	Kittitas Jail	Identix	Spillman	Y
1	Mason Jail	Visionics	Spillman	Y
1	Okanogan Jail	Visionics	Positron?	
1	Whitman Jail	Identix	Spillman	Y
<1	Jefferson Jail	Visionics	Abby	
*	Kitsap Juvenile	Visionics	JUVIS	
*	Olympia PD	Identix	New World	Y
*	Spokane Juvenile	Identix	JUVIS	
*	Sunnyside PD	Identix	Spillman	Y

* Included in county percentage

Operating Expenditures	**YEAR 1**	**YEAR 2**	**Total**
Equipment and Software	$690,000	0	$690,000

3) To further reduce paper fingerprint card submissions, the cost to acquire five (5) additional live-scan devices will be $150,000.

Yakima PD
Marysville PD
Pullman PD
Oak Harbor PD
Fife PD

Operating Expenditures	**YEAR 1**	**YEAR 2**	**Total**
Equipment and Software	$150,000	0	$150,000

Narrative Justification and Impact Statement

Local criminal justice agencies with a live-scan system connected to the state automated fingerprint identification system (AFIS) electronically submit fingerprints and related arrest information to facilitate real-time identification and timely inclusion in the criminal history data base.

The records management system (RMS) interfaces and replacements of end-of-life live-scan devices enhance efficiency and continue support to the local law enforcement

agencies. The opportunity to interface sites with the Spillman RMS at such a low cost will reduce a significant workload on the local agency and facilitate quicker submission and results.

The added cost and difficulty in maintaining older equipment will become burdensome for local law enforcement agencies. It may also result in more down-time, affecting their ability to identify offenders before their release back into the community. Electronic submission of fingerprints directly affects local and state workloads and provides a critical tool to law enforcement in the interest of public safety.

If funding is unavailable, staff will continue redundant data entry on systems with no RMS interface. Older equipment would need to be removed and the local agency would lose real-time identification of offenders, the criminal justice community and public would lose the benefit of timely and complete criminal history records, and the WSP would lose the efficiency of electronic arrest submissions.

How the Decision Package contributes to the applicant's strategic plan

Goal #3 – Leverage technology to improve business processes, systems, and statewide emergency communications interoperability.

How the Decision Package supports the JIN Mission and Objectives

This package supports the following JIN Objectives:

Improve workflow within the criminal justice system.
Provide complete, accurate, and timely information to criminal justice agencies.

How the Decision Package aligns with applicable grant requirements

This project aligns to the NCHIP program priority for "strengthening records to improve national security standards and avert terrorism." By providing the software and equipment necessary for law enforcement agencies to submit arrests electronically. Within this priority, this project further meets the following review criteria as outlined for the NCHIP program:

- Support/enhance participation in the NICS, III, the National Sex Offender Registry, the NCIC Protection Order File, the National Crime Prevention and Privacy Compact, and other related Federal and State systems: This project extends access to State and Federal arrest information to criminal justice agencies.

- The proposed use or enhancement of innovative procedures which may be of value to other jurisdictions: The results of this project will be available to all criminal justice agencies using criminal history record information.

- The technical feasibility of the proposal and the extent to which the proposal appears reasonable in light of the State's current level of system development and statutory framework: This live-scan equipment is proven technology within the state and

allows for enhancing current local systems, continuity of electronic arrest submissions for agencies with end-of-life devices, and expansion to increase electronic submissions.

- Reasonableness of budget: The budget for this project is based on other similar projects in Washington.

- Nature of the proposed expenditures: The expenditures to be funded under this application are those directly related to technology development required to connect and interact with the state and federal services.

- The reasonableness of the relationship between the proposed activities and the current status of the State system, in terms of technical development, legislation, current fiscal demands, and future operating costs: This project is in direct alignment to and partnership with the State's JIN Program.

Project Cost Alignment to NCHIP

The Washington State Patrol recommends $896,000 for this project, which is the portion of the overall project costs directly associated with live-scan interfaces, replacements, and acquisitions. The expenses for this project align to the following "allowable costs" for NCHIP:

- Participation in III: The project facilitates electronic arrest submission and entry in the state and federal automated fingerprint identification systems and criminal history data bases.

- Database enhancement: The project supports quality, completeness, and accuracy of criminal history record information to the state repository and the FBI NCIC III by improving the capture and submission of arrest and disposition information.

- Record enhancement and support of anti-terrorism and national security systems: The project expedites the submission of arrest information for real-time identification and criminal history record availability.

Attachment A: Project Management Plan, Schedule, and Performance Measures

Plan and Schedule

In the performance of technology projects, the Washington State Patrol (WSP) uses a system acquisition methodology. This project reports to the Washington State Office of Financial Management (OFM), which coordinates the purchase process, monitors monthly progress, and controls funding releases.

The high-level project plan with scheduled milestones for this project is as follows:

Install software interface..... July 30, 2005
Choose live-scan vendor for end-of-life replacements ..... August 30, 2005
Develop and test interface between live-scan and local systems..... September 30, 2005
Install replacement live-scan systems ..... June 30, 2006
Choose live-scan vendor for new acquisitions ..... August 30, 2005
Develop and test interface between live-scan and local systems..... September 30, 2005
Install new live-scan systems ..... June 30, 2006

The WSP works in coordination with OFM to evaluate and determine which vendor meets the software and hardware specifications and requirements. The WSP uses current resources for local site installation and training and provides OFM with regular project status.

Performance Measures

- Installation of interface software
- Number of end-of-life replacement live-scan systems installed to maintain an 80% electronic criminal history submission rate
- Number of new live-scan acquisitions to increase electronic criminal history submission by 8%